Bruteforced Directional Calibration in search of Nearest Neighbor (BDCNN) for Prevention of the Detection of Data Exfiltration by Multi-Node, Short-Range Sensor Networks and for Establishment of Relative Sensor Position in Support of Analytical Functions

1 August 2023
Simon Edwards
Research Acceleration Initiative

Introduction

The development of charge-state dependent EM-blocking metamaterials has opened the door to both highly direction-specific radio transmission as well as antenna sensitization (by dint of noise reduction) for intercept purposes. There are a variety of applications for the secure exfiltration of data captured from a contested environment where non-detection of the covert signal is mission-critical.

Some applications, such as that of using clusters of hundreds of proximity circuits to detect movement in urban environments, requires not only ensuring that the signal associated with the exfiltration of the relevant data is not detected, but that the exfiltrated data includes datapoints that can be used to extrapolate the relative position of the sensors in support of analytical tasks necessary to make appropriate use of the data.

Abstract

It is possible to undetectably exfiltrate data from multi-node sensor networks in contested environments using electromagnetism in the following way:

A sensor network consisting of near-microscopic sensor units could be dropped over a city by way of bomblet. These sensors would be coated with a sticky material that prevents their motion after finding a resting place on building roofs, roads and the walls of buildings. Any sensor near the perimeter of the contested area could be used by friendly forces as a point of exfiltration for the data prior to using a longer-range secure transmission system to exfiltrate data to a command post.

As it would be impossible to predict the position and orientation of the sensors in advance, the sensors would need to "find one another. They could not transmit signals in all directions lest they be detected. Upon deployment, in this novel system, the sensors would "bruteforce" through all possible relative transmission directions, with directional selectivity being made possible by a charge-state dependent metamaterial coating on the antenna. Microscopic portions of the coating could be selectively discharged in order to ensure broadcast of signals only in that particular direction, preferably at low-power.

All sensors in the network would be actively tracking their own orientation relative to magnetic north, triangulating received EM and even triangulating proximity circuit data depending upon the nature of the surveillance mission. If a compatible signal is received by a unit, a ping is returned in the appropriate direction. When a unit in this network "finds" a neighbor in this way, it semi-permanently affixes its direction of transmission in the direction of the "found" neighbor. Each sensor/transmitter in the network would mutually conduct this calibration process so that data would attempt to reach the perimeter of the network through as many pathways as possible.

Provided a directional specificity of transmissions of 1/10th of one degree of angle, a network of nodes covering an area of one square mile in which none of the signals have a range of more than 30 feet would be detectable from only 1/50,000th of the surface area in question, making detection of the covert exfiltration network highly unlikely.

Conclusion

BDCNN combines the advantages of collimated beam communications protocols and short-range covert transmission with the added advantage of a self-calibrating capability in a near-microscopic form factor. This approach falls within the current SotA and thus may be prototyped and tested at relatively low cost with substantial potential benefits.